BAB V

PENUTUP

Pada bab ini penulis akan membahas kesimpulan dan saran yang diperoleh dari hasil pembahasan pada bab-bab sebelumnya. Kesimpulan akan diuraikan dari proses analisis vulnerability dan pembuktian hipotesis. Kemudian saran akan disampaikan sebagai usulan dan masukan untuk peneliti berikutnya.

5.1 Kesimpulan

Mengamati penjelasan dan pembahasan dari penelitian berjudul "Testing Penetrasi Server Proxy Pada Warnet Galeri Informatika Kecamatan Semin Kabupaten Gunungkidul", maka dapat diambil kesimpulan sebagai berikut.

1. Tujuan penelitian tercapai. Kegiatan testing penetrasi menggunakan metode *Penetration Testing Execution Standard* (PTES) berhasil dilakukan untuk analisis keamanan jaringan, khususnya server proxy di Warnet Galeri Informatika.
2. Empat dari lima hipotesis tidak terbukti. Penulis dapat membuktikan hipotesis kerentanan LAN secara fisik, namun tidak berhasil membuktikan hipotesis kerentanan sistem pada server proxy.
3. Adapun celah keamanan terdapat pada pengelolaan LAN secara fisik. Hipotesis kerentanan berupa penyalahgunaan hak akses pengguna, telah terbukti pada sub bab 4.1.1.
4. Rekomendasi untuk memperbaiki kondisi yang terbukti rentan, telah disampaikan penulis pada sub bab 4.2.4.

5.2 Saran

Berdasarkan evaluasi terhadap analisis kerentanan dan pembuktiannya melalui testing penetrasi, maka saran penulis untuk pengembangan dalam penelitian selanjutnya adalah sebagai berikut.

1. Peneliti selanjutnya dapat membuat skenario analisis kerentanan dan percobaan serangan dari luar LAN. Hal ini berguna untuk testing kekuatan router atau perangkat lain.
2. Peneliti selanjutnya dapat melakukan kegiatan testing penetrasi dengan metode selain PTES, misalnya *National Institute of Standard Technology* (NIST) *guideline in network security*. Tujuannya untuk membandingkan metode yang tepat dan efisien jika diterapkan untuk kasus serupa.
3. Untuk testing penetrasi dengan lingkup yang lebih luas, misalkan sistem informasi manajemen, metode lain yang dapat dipakai adalah *Open Web Application Security Project* (OWASP). Selain itu juga ada *Offensive Web Testing Framework* (OWTF) untuk sistem berbasis web.